EXHIBIT C

Application Report
SLUA346–July 2005

Battery Authentication and Security Schemes

Portable Power Battery Management Applications

ABSTRACT

Driven by integrated functionality and shrinking form factors, the demand for portable devices, such as cellular phones, PDAs, and DVD players, has grown significantly during the last several years. These portable devices need rechargeable batteries and peripherals that must be replaced before the life of the portable devices expires. This has opened a huge market for counterfeiters to supply cheap replacement batteries and peripherals, which may not have the safety and protection circuits required by the original equipment manufacturer (OEM).

These counterfeit batteries may violate both mechanical and electrical safety requirements related to short-circuit protection, charge safety, and other specifications. It is usually impossible for the consumer to determine the quality without making a purchase and possibly learning the hard way. This can lead to a potentially dangerous situation for end-users. Adding simple and effective authentication technology to the portable system allows the OEMs to ensure customer satisfaction and to protect their businesses. More importantly, safety is guaranteed throughout the life of the product.

This application report discusses in detail the simple identification (ID) and the more complicated challenge and response CRC and SHA-1/HMAC-based battery authentication schemes. The presented battery authentication architectures meet the counterfeit battery challenges to protect OEM businesses and to ensure end-user safety and satisfaction.

Contents

List of Figures

1 Identification-Based Authentication Scheme

Several authentication schemes currently are used to identify that a battery pack is intended for specific portable products. The most common is the form factor or physical connection. Every cell phone battery pack on the market has a different form factor. However, the physical size of the battery pack is not even consistent within all phones manufactured by the same company. Whereas this method of identification

affords some level of protection for low-volume manufacturers, batteries from manufacturers with high volumes are much more likely to be counterfeited. It would be an inexpensive solution to standardize form factors and keep them unchanged. Many OEMs are moving toward this economic model. However, this provides an opportunity for counterfeiters to replicate the battery pack by measuring the physical dimension.

To improve battery identification, an electrical identification scheme could be used so that simple physical counterfeiting is no longer enough to replicate the battery. Figure 1 shows the ID authentication functional block diagram. The challenger or host sends a command to read the data from the device (responder). The data include product family code, identification number (ID), and cyclic redundancy check (CRC) value. Each device has a unique ID number. The response data is compared with the data in the host. If the data from the device is valid, then the host allows enabling the system operation. Otherwise, it inhibits the system operation and provides an error code and a warning signal to the end-user. Integrated circuits (IC) such as the bq2022 and bq2023 provide a unique ID for each device. Figure 2 shows the battery pack typical application circuit with the ID chip. The host communicates with the chip through a dedicated general-purpose I/O to determine if an ID is available and valid. The ID authentication scheme eliminates a significant number of non-OEMs. However, the ID issued by the device is available to anyone with an oscilloscope. It is still possible for the counterfeiters to replicate the ID to the issued command. But, it increases the cost to implement a fake ID. Even so, some non-OEMs still go after batteries and peripherals for high-volume products and adding a cheap microcontroller to the system is acceptable to them. To counter this threat, a more robust authentication scheme is required.

2 Challenge and Response-Based Authentication Scheme

A straight ID authentication increases the complexity for the counterfeiter to identify the ID and the command. It is secure by adding cost to the system. If cost is important, a non-OEM will opt for a battery or peripheral without this functionality. But for those non-OEMs that are willing to add cost to their system to secure a business opportunity, something more robust than an ID authentication is needed.

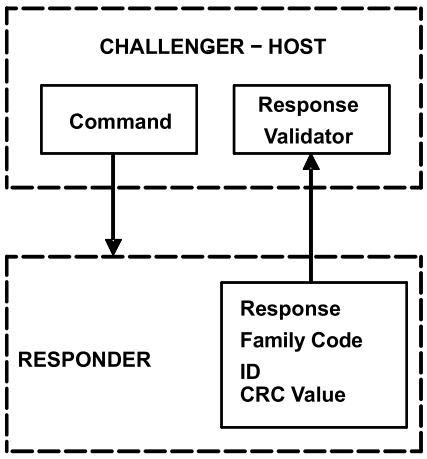

Figure 1. ID Authentication Functional Block Diagram

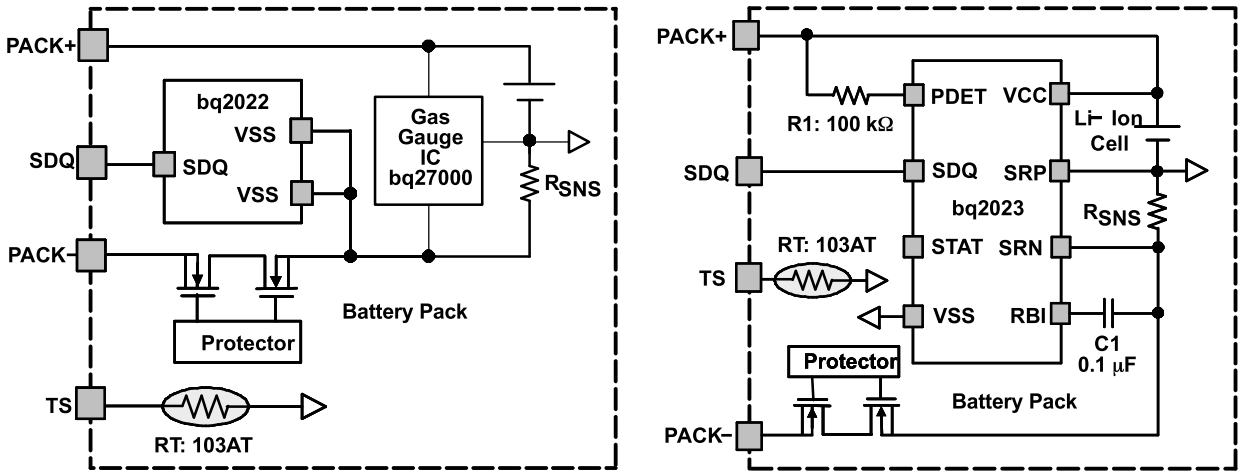

Figure 2. Typical Application Circuit With ID Chip

A more cost-effective and robust approach is based on a challenge and response scheme as shown in Figure 3. In this scheme, the host sends a random challenge to the battery pack that contains the identification device, or responder. The random challenge consists of a number of bits of random data generated by the host. The secret key is either shared or transmitted securely from one side to another. When the authentication device receives the challenge information, it performs the authentication transform with the plain-text key stored in the private memory of the device to calculate the response. On the other side, the host performs the same transform using the plain-text key generated by the secret key from the host and the encrypted key from the device. The result compares the value it computes against the response obtained from the identification device. If the calculated data from the authentication device matches the expected answer from the host, then the host authenticates the battery and allows the system to start operation. Otherwise, it may inhibit the system operation and provide a warning signal to the end-user.

Why is this scheme more secure than the straight ID-based scheme? The single ID authentication scheme has a fixed response to a fixed challenge or command. It is relatively easy for counterfeiters to find out the fixed challenge and command. However, the challenge and response secure scheme changes the query and response every time. A relatively large and random challenge makes a look-up table solution expensive in terms of memory. It has a direct correlation with the monetary cost and is difficult to guess. In addition, part of the transform involves a secret key shared between the challenger and the responder. Security then resides in the secret key, allowing the scheme to use a public authentication transform algorithm. Public authentication transforms are effective because they can be thoroughly and properly evaluated for robustness against attacks seeking to uncover the secret key.

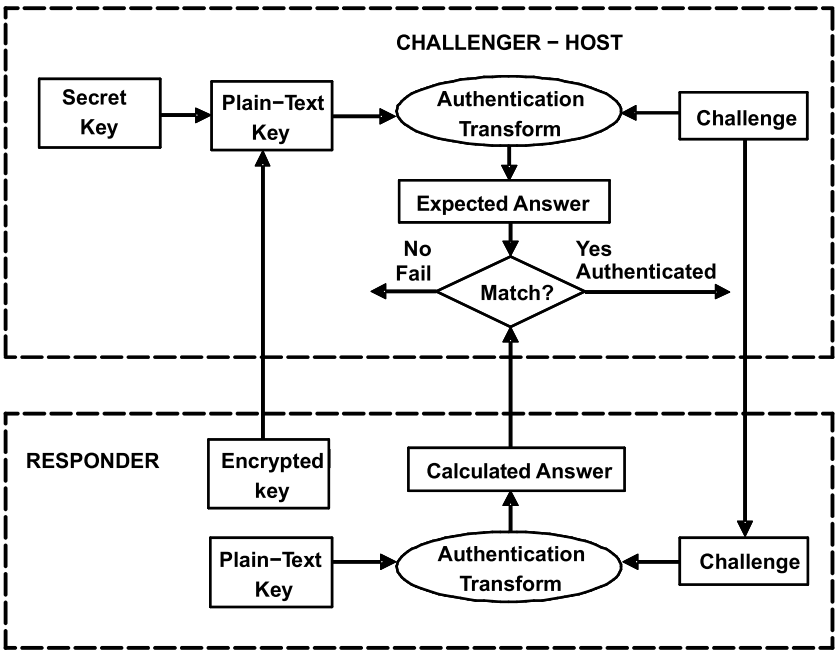

Figure 3. Challenge and Response-Based Authentication Scheme

3 Challenge and Response CRC-Based Authentication Implementation

Figure 4 shows the CRC-based authentication implementation diagram based on the concept of challenge and response authentication scheme previously discussed. The authentication transform uses CRC to calculate the value to authenticate the battery pack. It combines a 32-bit challenge and a 96-bit secret ID through a CRC with a random polynomial and seed value to generate a 16-bit CRC response. Security is achieved through the use of a 16-bit CRC, a 16-bit CRC seed, a 96-bit device ID, and a 32-bit random challenge. The CRC polynomial, CRC seed, and 96-bit ID are unique from device to device. They are stored as encrypted text in public memory and as plain text in private memory. Any external device cannot access the private memory to look at the plain text of the CRC polynomial, CRC seed, and ID. The host system can decrypt the polynomial, seed, and ID values using the secret key that is stored in the end-equipment's memory. The encryption method and the secret key used to store the polynomial coefficients and the device ID can be selected by the manufacturer. To authenticate a battery pack, the host reads the encrypted device ID, polynomial, and seed values from the public memory. It decrypts those values using the secret key and then generates a 32-bit random challenge. The generated random challenge is transmitted to the authentication device, which uses the plain-text version of the polynomial coefficients, seed, and device ID, along with the 32-bit random challenge from the host to calculate the authentication CRC value. The host uses the polynomial coefficients, seed, and device ID that it decrypted, along with the 32-bit random challenge that it sent to the authentication device to calculate the authentication CRC value.

When the host and the authentication device have completed the calculation, the host reads the authentication CRC value from the authentication device and compares it to its own value. If the values match, the battery pack is authenticated. The host can initiate the system start command, and it is allowed to communicate with other devices in the battery pack such as the gas gauge. Otherwise, the host may not initiate the system start-up command and provide a warning signal to the end-user. Figure 5 shows the battery pack typical application circuit with CRC-based battery authentication. The authentication chip has an internal regulator powered by the communication line, and it can communicate to the gas gauge IC. If the authentication fails, the host may not allow charging the battery and provides a warning signal to the user. The CRC-based authentication provides a simple and cost-effective solution to authenticate battery packs for end-equipment.

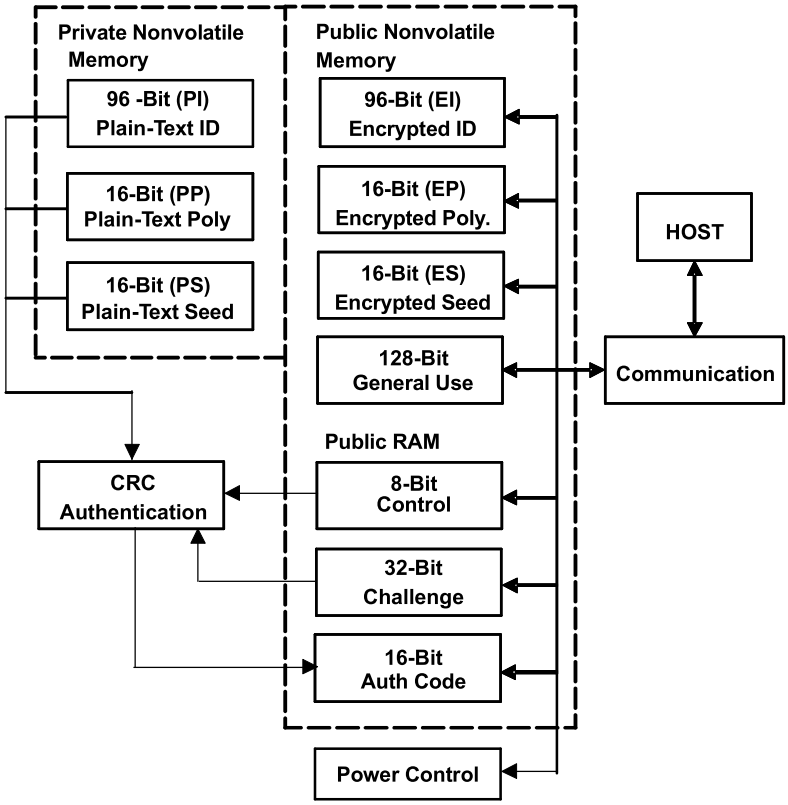

Figure 4. Challenge and Response CRC-Based Authentication Block Diagram

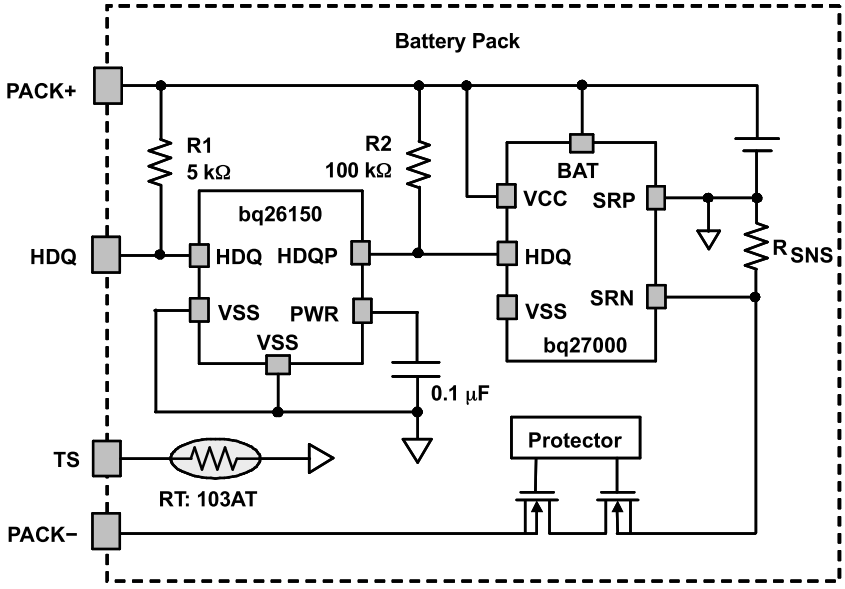

Figure 5. Battery Pack Typical Application Circuit With CRC-Based Authentication Chip

4 Challenge and Response SHA-1-Based Authentication Implementation

In order to achieve a high level of authentication, a more sophisticated algorithm such as the SHA-1/HMAC secure hash algorithm can be used. The SHA-1/HMAC has been used for years to authenticate Internet transactions for Virtual Private Networks, banking, and digital certificates. The algorithm used in SHA-1/HMAC is iterative. One way hash functions can process a message is to produce a condensed representation called a message digest. It enables the determination of a message's integrity. Any change to the message results in a different message digest with a high probability. This property is useful in the generation and verification of digital signatures and message authentication codes. Figure 6 shows the block diagram of SHA-1/HMAC-based authentication. The authentication principle is similar to the CRC-based scheme except that the algorithm is different. To authenticate a battery pack, the host reads the 128-bit encrypted device ID from the public memory. It decrypts those values using the secret key to achieve the plain-text information with root keys. It then generates a 160-bit random challenge. The generated random challenge is transmitted to the authentication device, which uses the plain-text version of the ID along with the 160-bit random challenge from the host to calculate the authentication digest value. The host uses the decrypted ID along with the same 160-bit random challenge that is sent to the authentication device to calculate the authentication digest value. When the host and the authentication device have completed the calculation, the host reads the authentication digest value from the authentication device. It then compares it to its own value. If the values match, the battery pack is authenticated. Otherwise, the host may not initiate the system start-up command or provide a warning signal to the end-user. Because there is a 160-bit random challenge, it generates 2^{160} possibilities. This significantly improves the security level. However, the SHA-1/HMAC algorithm requires more memory size, which increases the cost.

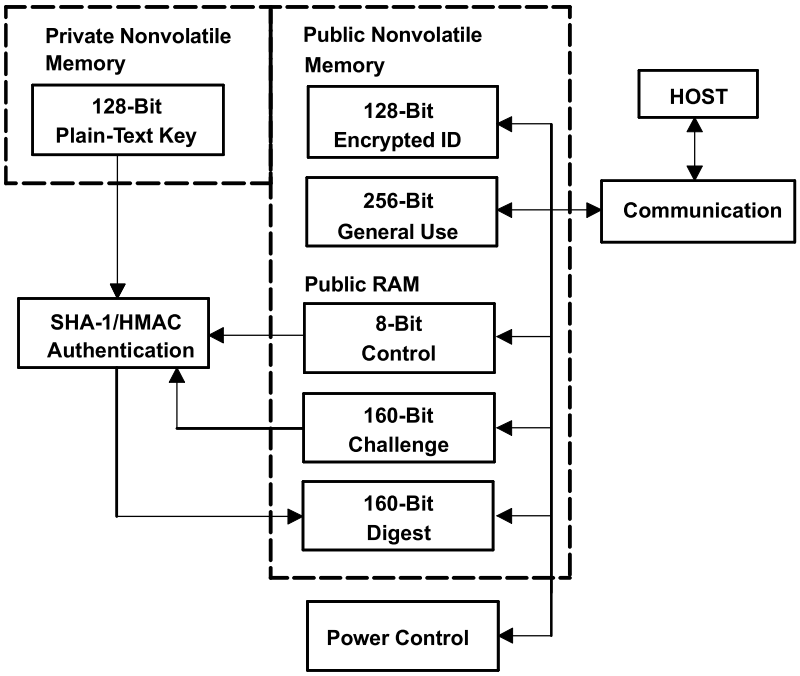

Figure 6. Challenge and Response SHA-1/HMAC-Based Authentication Block Diagram

5 Summary

The selection of the battery authentication scheme among the simple ID authentication, CRC-, and SHA-1/HMAC-based authentication depends on the security level needed and cost for the applications. The simple ID authentication is the least expensive and is good for cost-sensitive applications, but it is easy to replicate . Although the challenge and response CRC- and SHA-1/HMAC-based authentications are the most expensive, they have the highest security and are good for the high-end portable applications.

IMPORTANT NOTICE

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, modifications, enhancements, improvements, and other changes to its products and services at any time and to discontinue any product or service without notice. Customers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All products are sold subject to TI's terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its hardware products to the specifications applicable at the time of sale in accordance with TI's standard warranty. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by government requirements, testing of all parameters of each product is not necessarily performed.

TI assumes no liability for applications assistance or customer product design. Customers are responsible for their products and applications using TI components. To minimize the risks associated with customer products and applications, customers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any TI patent right, copyright, mask work right, or other TI intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information published by TI regarding third-party products or services does not constitute a license from TI to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. Reproduction of this information with alteration is an unfair and deceptive business practice. TI is not responsible or liable for such altered documentation.

Resale of TI products or services with statements different from or beyond the parameters stated by TI for that product or service voids all express and any implied warranties for the associated TI product or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Following are URLs where you can obtain information on other Texas Instruments products and application solutions:

Products		**Applications**	
Amplifiers	amplifier.ti.com	Audio	www.ti.com/audio
Data Converters	dataconverter.ti.com	Automotive	www.ti.com/automotive
DSP	dsp.ti.com	Broadband	www.ti.com/broadband
Interface	interface.ti.com	Digital Control	www.ti.com/digitalcontrol
Logic	logic.ti.com	Military	www.ti.com/military
Power Mgmt	power.ti.com	Optical Networking	www.ti.com/opticalnetwork
Microcontrollers	microcontroller.ti.com	Security	www.ti.com/security
		Telephony	www.ti.com/telephony
		Video & Imaging	www.ti.com/video
		Wireless	www.ti.com/wireless

Mailing Address: Texas Instruments
Post Office Box 655303 Dallas, Texas 75265